



# Risk-based Design for Heavy Industry

Hosted by the Electrical Energy Society of  
Australia (EESA)

Presented by David Hawkins

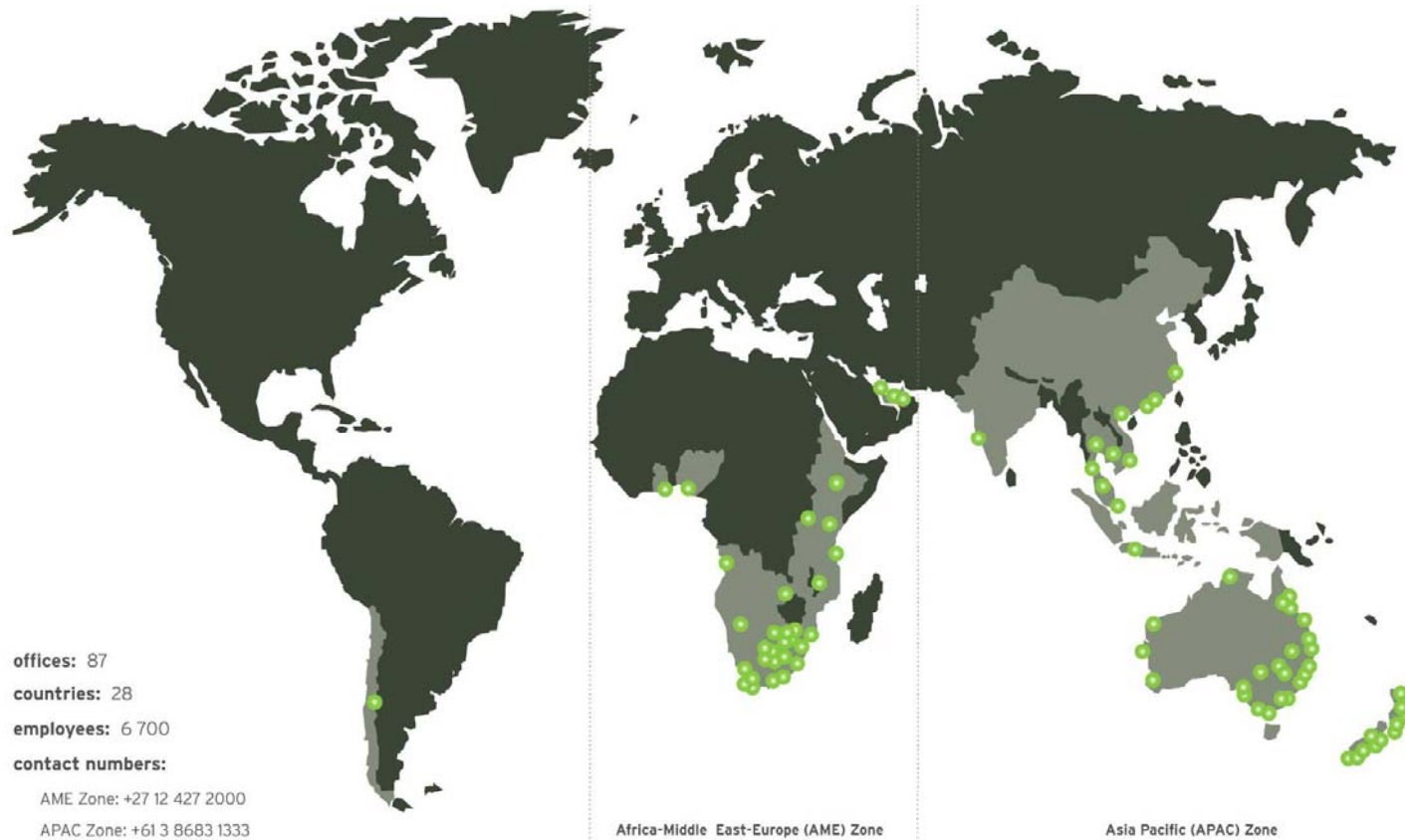
10 August 2009



 **aurecon**



**Leading. Vibrant. Global.**



Risk-based Design for Heavy Industry  
10 August 2009

# Introduction

## What is to be presented

- What is risk based design
- State regulations, national guidelines and standards
- Risk assessment process
- Tolerable risk
- Integrity of a safety instrumented function
- Approach to the design of safety instrumented systems

# What is risk based design

An example of why



Figure Showing GP 905 Heat Exchanger of Longford Gas Plant

From: The 50 Major Engineering Failures (1977-2007)

<http://integrityengineering.wordpress.com>

# What is risk based design

## Context (OHS&W)

- Technical risk associated with plant
- Protect the health and safety of persons from hazards
- Duties of: designers, manufacturers, importers, suppliers, erectors or installers, employers, and owners
- On the basis of a risk assessment ... ensure that any risks to health or safety arising out of work are eliminated or, where that is not reasonably practicable, minimised
- Firstly, the application, where is reasonably practicable, of engineering controls, including substitution, isolation, modifications to design
- Provision of information
- Emergency stops...as far as reasonably practicable operate reliably and be fail-safe

# What is risk based design

## Some examples of where

- Heavy industry
- Manufacturing
- Power generation
- Mining
- Process
- Petrochemical



# What is risk based design

## Key Features

- Performance based standards apply
- An instrumented system is required to reduce the risk to broadly tolerable
- The following items are carefully selected or designed to improve integrity
  - Equipment selection
  - Voting architecture
  - Installation techniques
  - Proof testing (low demand systems)

# Regulations, Guidelines and Standards

## Key examples of Regulations, Guidelines and Standards

- Regulations – OHS&W, Gas, Petroleum, Dangerous Substances, Environment Protection, Electricity
- Guidelines – NOHSC MHF ([www.safeworkaustralia.gov.au](http://www.safeworkaustralia.gov.au)), NSW Planning guidelines HIPAP & NFPA 85: Boiler and Combustion Systems Hazards Code
- Standards – AS/NZS 4360 Risk Management, AS 1755 Conveyor safety, AS 1418 Cranes, AS 3814 Gas-fired appliances, AS IEC 61508 Functional safety, AS IEC 61511 Functional safety for process sector, AS 4024 Machine safety, AS 60261 Functional safety for machines

# Regulations, Guidelines and Standards

## South Australian OHS&W Regulations

... the identification of hazards and the assessment of associated risks must be undertaken—

- a) before the introduction of any plant or substance
- b) before the introduction of a work practice or procedure
- c) before changing the workplace, a work or work practice, or an activity or process, where to do so may give rise to a risk to health or safety

Clause 1.3.2 sub-regulation (4)

# Regulations, Guidelines and Standards

## Relationship of Regulations to Standards

- Gas Regulations 1997
  - Calls AS 3814 Gas appliances
  - AS 3814 refers to AS 61508 Functional Safety
- Occupational Health, Safety and Welfare Regulations 1995
  - Calls AS 1755 Conveyor Safety and AS 1418 Cranes
  - These standards call AS 4024 Safety of Machinery
- [SA Legislation and Standards Block Diagram](#)

# Risk assessment process

## Preferred processes

- Safety in Design
- HAZOP
- CHAZOP
- Machine Safety

## Alternative processes

- Checklist
- What if study
- FMEA

# Risk assessment process

## Safety in Design

- Workshop approach using checklist and what-if study techniques
- Suited for reviewing
  - Civil and structural design projects
  - Substation and transmission line projects
  - Constructability and broad hazards for plant
  - Where plant and hazards are generally well understood from past experience
- Qualitative approach, susceptible to psychological traps; anchoring, status quo, sunk-cost, calibration, complacency, paranoia

# Risk assessment process

## HAZOP – Hazard Operability Studies

- HAZOP workshops to AS 61882 and Orica guidelines
- Systematic approach for identifying hazards
  - Workshop participants are selected for specific roles and expertise
  - Logical breakdown of plant under review
  - Prompts used to reveal deviations from normal process conditions
  - Cause, consequence and safeguards systematically recorded
  - Actions and further analysis can be determined as an outcome
- Suited for reviewing
  - Piping and instrumentation diagrams
  - Materials flow diagram
  - Traffic flow

# Risk assessment process

## CHAZOP – Control Hazard Studies

- Similar process to a HAZOP with a controls and instrumentation focus
- CHAZOP usually follows on from a HAZOP
- Investigates potential systematic errors of the control system and related hazards
- Control and trip system investigated
  - Does loss of control functionality lead to potential hazards?
- Top down and bottom up approaches use different prompts
- Typical inputs to CHAZOP include
  - Previous risk assessments, functional specifications
  - Process flow diagram, single line diagram
  - General arrangements, details of control room

# Risk assessment process

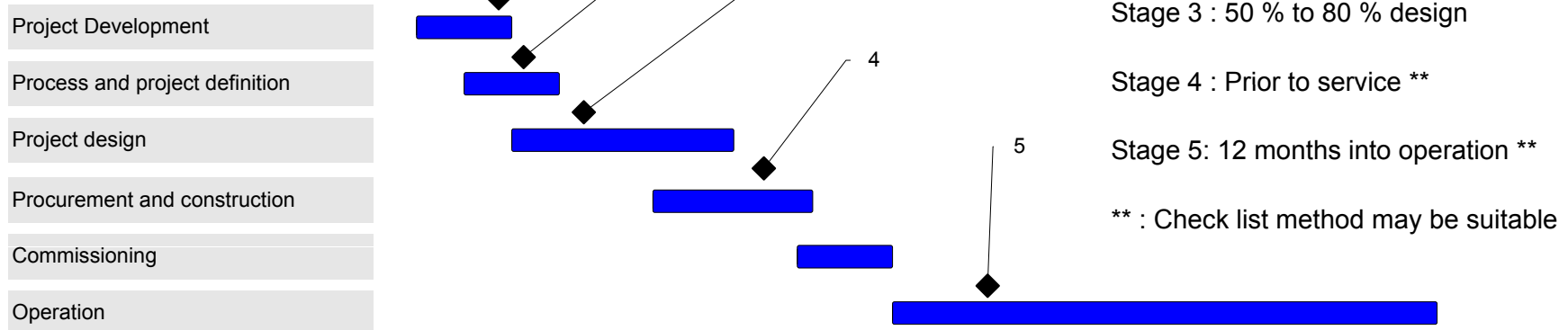
## Machine safety

- Machine safety to AS4024 series
- Similar process to a HAZOP with a machine focus (conveyors, cranes and machines)
- Determines requirements for
  - Emergency stops
  - Guarding
  - Access interlocking
- Suited for reviewing
  - Materials flow diagram
  - Conveyor, crane or machine arrangements
  - Mobile machines and cranes

# Risk assessment process

## Approach and Schedule

- Top down and bottom up approach
- Five stages



# Risk assessment process

## Qualitative:

Checklist  
What If  
Safety In Design  
Top Down HAZOP

- Initial risk process for plant
- Hazards tend to lower consequence higher frequency
- Hazards can be mitigated to a broadly tolerable level without implementing instrumented controls
- Covers constructability hazards that can be adequately designed out

## Semi-Quantitative:

Bottom up HAZOP  
Machine Safety Risk Assessment

- Piping and Instrumentation Diagram review
- Materials Flow Diagram review
- Suitable for traffic flow review
- Conveyer code applies (AS 1755)
- Crane code applies (AS 1418)
- Hazards tend to higher consequence
- Instrumented controls required

## Quantitative:

HAZOP (strict historical data & mathematical relationships)  
Consequence Analysis  
Likelihood Analysis  
Event Tree Analysis  
Layer of Protection Analysis  
Safety Requirements Specification

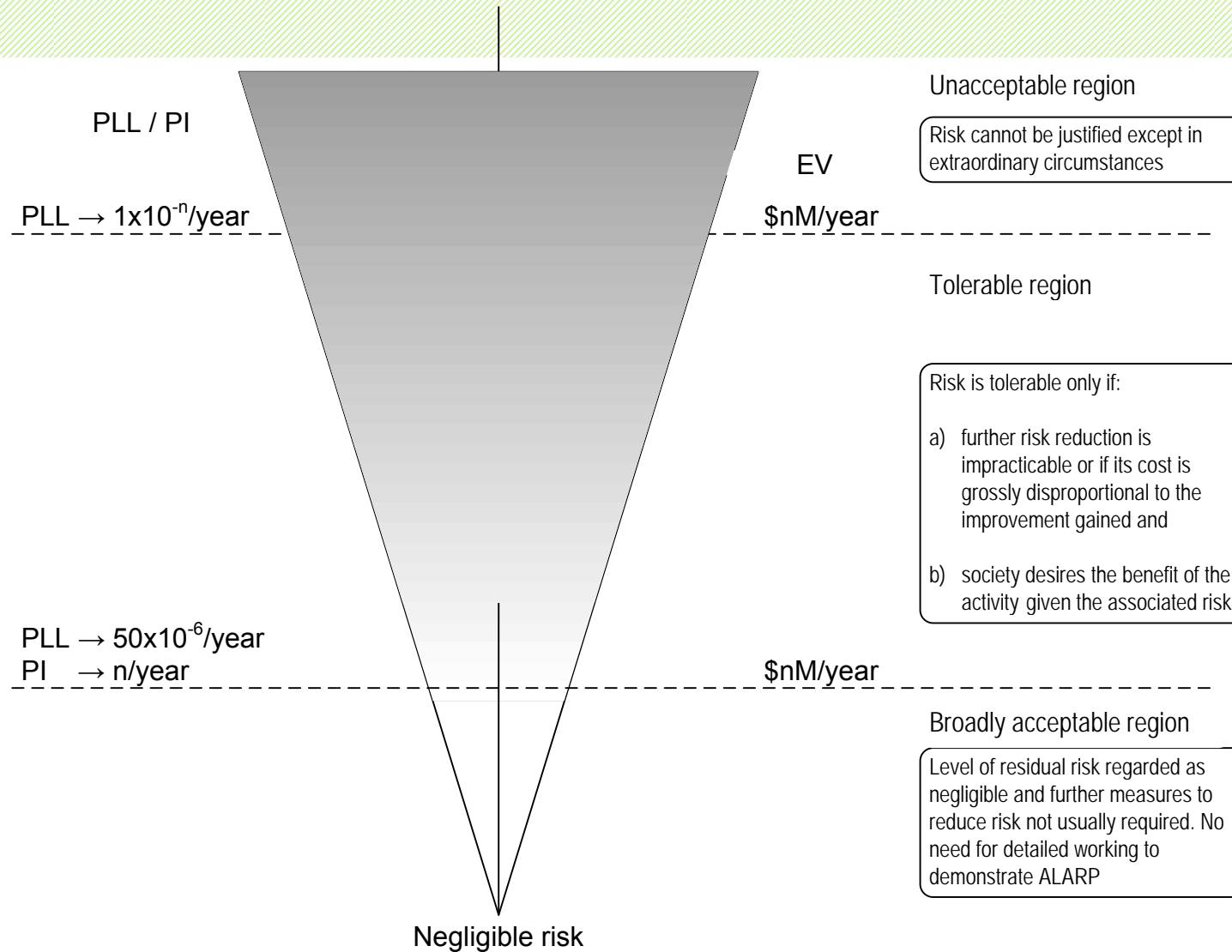
- Industrial and commercial gas-fired appliances AS (3814)
- Pipelines-Gas and liquid petroleum (AS 2885)
- Trip or protection system exceed Criteria II
- Regulatory requirement for quantified assessment
- Complex system noted in AS 4024
- SIF in range of SIL 1 and SIL 3
- SIF in range of RRF 10 and 10,000
- AS IEC 61508 series applies (AS4360 principles apply)

# Tolerable risk

## Introduction

- Moral, legal and financial responsibility to limit risk
- Provide a clear appreciation of risk
- Provide an appreciation of quantified and semi-quantified risk analysis
- Define the tolerable risk of an organisation in context of applicable regulations and standards
- ALARP
- Features of a calibrated risk matrices
- Consequence and Likelihood relationship

# Tolerable risk



# Tolerable risk

## Features of a calibrated risk matrices

- Site risk matrices should be calibrated with consideration of: corporate risk policy, Government planning guidelines and site / process characteristics
- Consequence and likelihood, increment by orders of magnitude
- Risk integrals, Probable Loss of Life (PLL) and Expected Value (EV)
- ALARP for PLL and EV are likely to result in separate risk matrix for each
- SIF risk matrices should be developed from a recalibrated site risk matrices
- Three clear risk regions matching ALARP
- Final tolerable risk report should be in context of appropriate standards and purpose
- Final tolerable risk report should be agreed by appropriate corporate representative

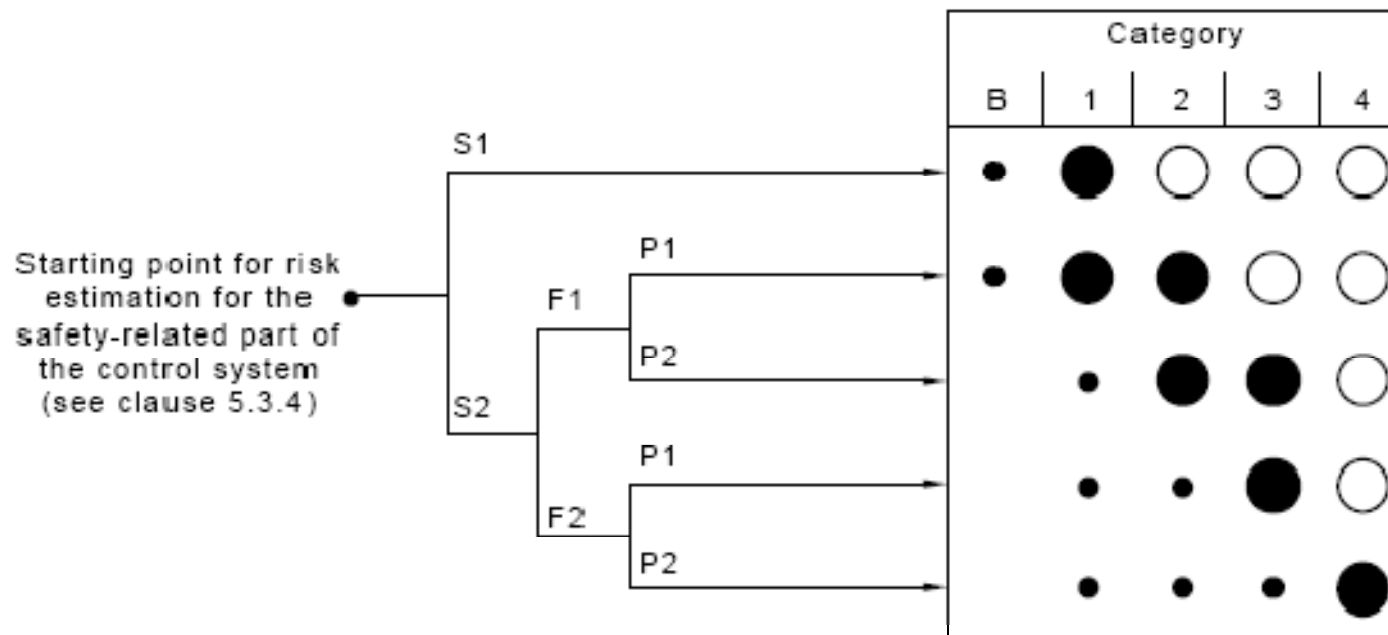
# Tolerable risk

## Example of a calibrated risk matrix

Consequence	Minor	Moderate	Major	Severe	Critical
Production Loss / Asset Damage	\$1,000 - 10,000	\$ 10,000 - \$100,000	\$ 100,000 - \$1 million	\$1 million - \$10 million	\$10 million - \$100 million
Likelihood	Risk				
Definite (> once per year)	\$ 10,000 to \$ 100,000	\$ 100,000 to \$ 1 million RRF: 10 to 100	\$ 1 million to \$ 10 million RRF: 100 to 1,000	\$ 10 million to \$ 100 million RRF: 1,000 to 10,000	\$ 100 million to \$ 1 billion RRF: 10,000 to 100,000
Almost certain (once per year)	\$ 1,000 to \$ 10,000	\$ 10,000 to \$ 100,000	\$ 100,000 to \$ 1 million RRF: 10 to 100	\$ 1 million to \$ 10 million RRF: 100 to 1,000	\$ 10 million to \$ 100 million RRF: 1,000 to 10,000
Likely (1 in 10 years)	\$ 100 to \$ 1,000	\$ 1,000 to \$ 10,000	\$ 10,000 to \$ 100,000	\$ 100,000 to \$ 1 million RRF: 10 to 100	\$ 1 million to \$ 10 million RRF: 100 to 1,000
Unlikely (1 in 100 years)	\$ 10 to \$ 100	\$ 100 to \$ 1,000	\$ 1,000 to \$ 10,000	\$ 10,000 to \$ 100,000	\$ 100,000 to \$ 1 million RRF: 10 to 100
Very Unlikely (1 in 1,000 years)	\$ 1 to \$ 10	\$ 10 to \$ 100	\$ 100 to \$ 1,000	\$ 1,000 to \$ 10,000	\$ 10,000 to \$ 100,000

# Tolerable risk

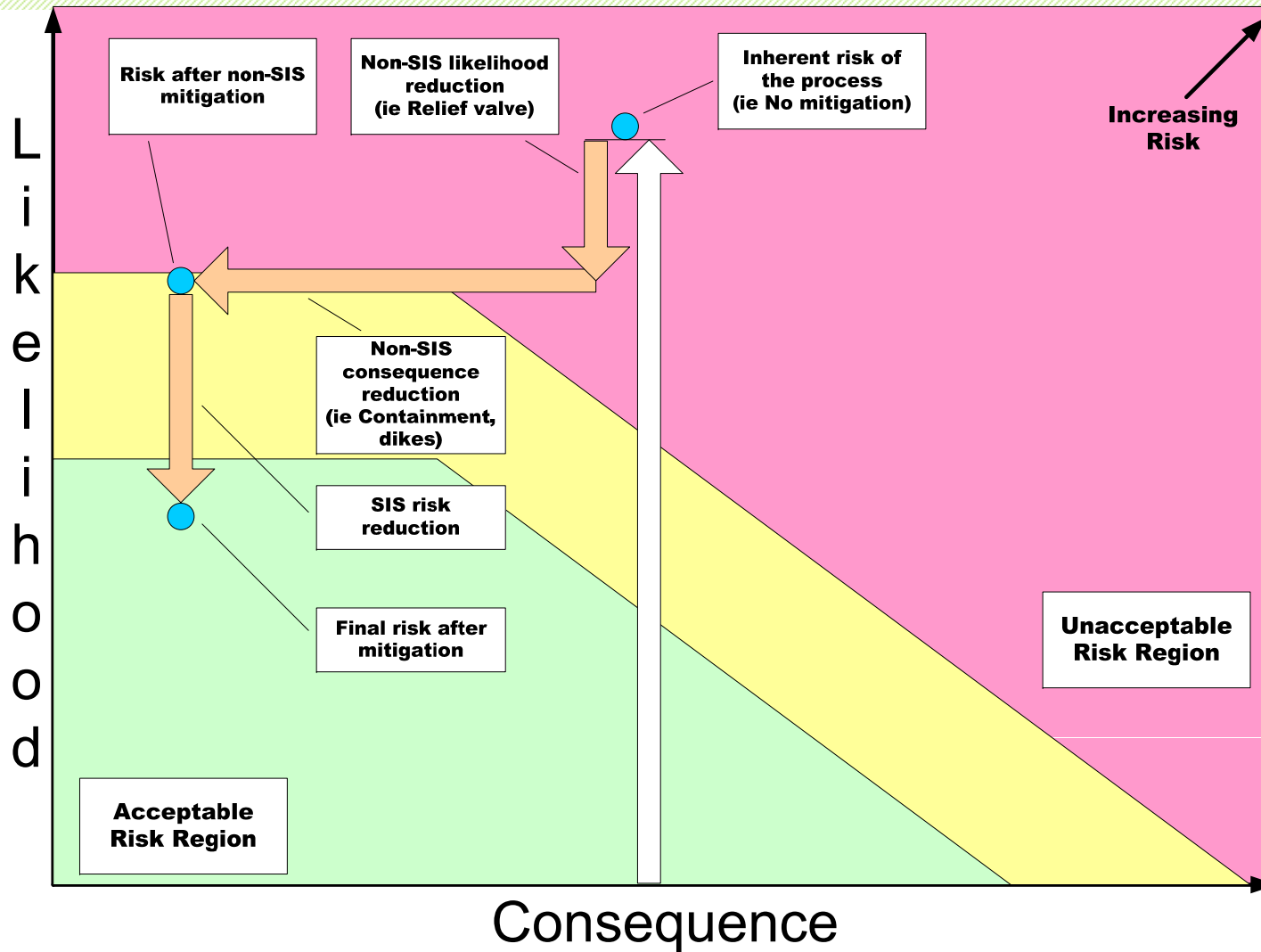
## AS 4024 risk graph (semi-quantified risk analysis)



Selection of categories B, 1 to 4

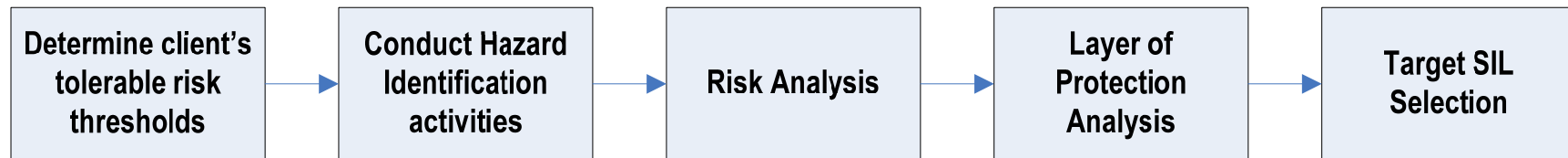
- = Preferred categories for reference points (see clause 5.2)
- = Possible categories which may require additional measures (see paragraph C1)
- = Measures which can be over-dimensioned for the relevant risk

# Tolerable risk



# Integrity of a Safety Instrumented Function

## Analysis phase process



# Integrity of a Safety Instrumented Function

## SIL based design

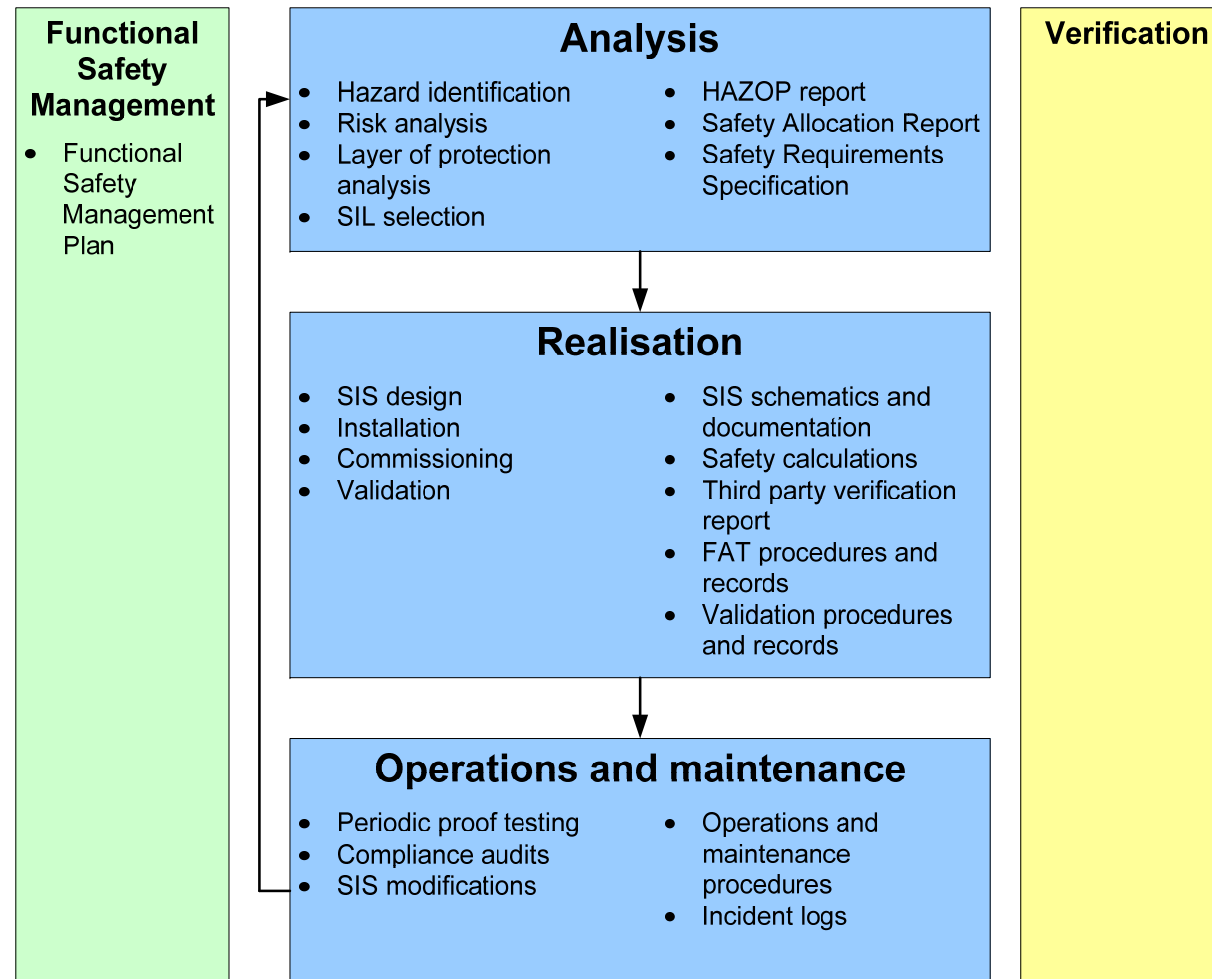
- Follow the requirements of AS 61508, AS 62061 and AS 61511
- Safety Integrity Level (SIL) from 1 to 4
- Each SIL corresponds to a risk reduction factor
- Performance based design that includes consideration of the customer's tolerable risk

## Category based design

Applies to process industry and complex machine applications

- Follow the requirements of AS 4024
- Categories of design from B and from 1 to 4
- Category selection based on assessment of severity of harm, frequency of exposure and probability of avoidance
- Applies to simple machine safety applications

# Approach to the design



# Approach to the design

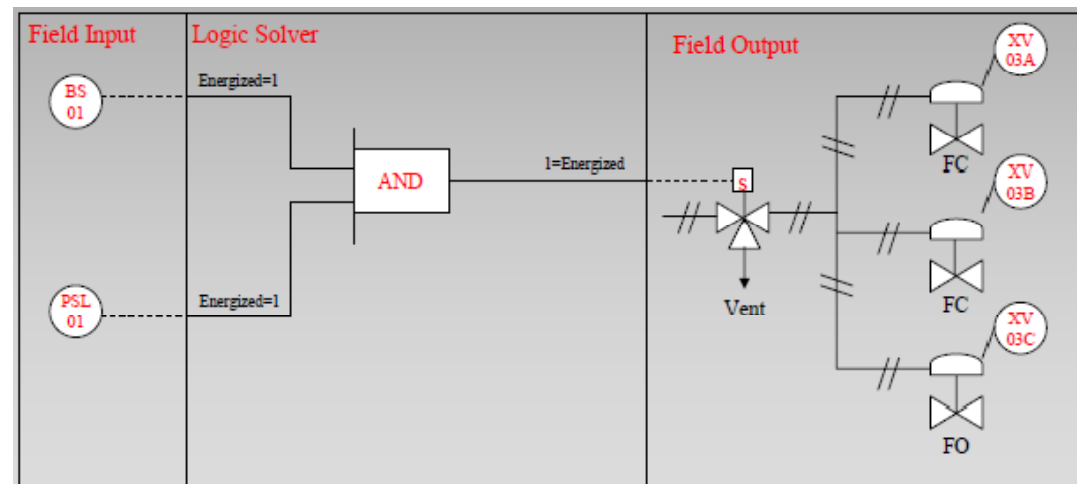
## Analysis phase

- Hazard identification
- Risk assessment
  - Definition of clients safety targets / tolerable risk
  - Likelihood analysis
  - Consequence analysis
- Layers of protection analysis
  - Assign risk reduction to other layers of protection
  - Determine necessary risk reduction required by SIS
- Good analysis will avoid an over-engineered safety system but still provide the required level of protection

# Approach to the design

## Analysis phase – Safety Requirements Specification (SRS)

- Specifies both the functional and integrity requirements
- Functional requirements
  - Sensors, logic, actuators
  - Response time
  - Energize/de-energize to trip
  - Definition of the safe state
- Integrity requirements
  - SIL
  - Demand rate
  - Proof testing requirements
  - Diagnostics
  - Maximum spurious trip rate



SRS is a key document for design, commissioning, maintenance and operation

# Approach to the design

## Realisation phase – SIS design

- Design of the safety instrumented system (SIS)
  - Hardware fault tolerance
  - Selection of equipment
  - Application software design and development
- Installation
- Commissioning and validation
  - Validation planning
  - FAT
  - Site validation testing
- Independent functional safety assessment required before placing into service



# Approach to the design

## Operations and maintenance phase

- Operate in accordance with the SRS
- Periodic proof testing
  - Failure data feeds back into lifecycle
- Modifications
  - Must be properly planned, reviewed and approved
  - Required SIL is maintained
  - Redo Safety Lifecycle steps for the modifications
- Compliance audits
  - Is the system being operated in accordance with SRS?
  - Are there discrepancies between actual and expected behaviour?

# Approach to the design

## Key features of a Safety Instrumented System

- Separation
- Systematic errors effectively removed
- Certified equipment or equipment of known appropriate characteristics
- SIS generally supervises until the safety function is demanded
- Safety life cycle processes are implemented

# Functional safety project example

## Onesteel Pellet Plant Kiln BMS Upgrade

**Location:** Whyalla, South Australia

**Completion date:** February 2008

### **Aurecon's services & solutions:**

- Safety instrumented system design and realisation
- Safety PLC and SCADA design
- Commissioning
- Project management

### **Interesting facts & figures:**

- Kiln produces 2 million tonnes of iron pellets annually
- Project commissioned in scheduled down times to minimise production losses



# Functional safety project example

## Eraring Energy Turbine Upgrade

**Location:** New South Wales

**Completion date:** in progress

**Aurecon's services & solutions:**

- SIL selection for turbine trip functions
- Risk assessment facilitation
- Safety requirements specification

**Interesting facts & figures:**

- Yokogawa Electro-hydraulic governor is the first to be implemented on a turbine this size



- Thankyou
- Questions

**Close**

**SA Occupational Health, Safety and Welfare Act 1986**  
Part 3 — General provisions relating to occupational health, safety and welfare  
Section 19 — Duties of employers  
Section 22 — Duties of employers and self-employed persons

**Occupational Health, Safety and Welfare Regulations 1995**  
Clause 1.3.2 — Hazard identification and risk assessment  
Clause 1.3.3 — Control of risk  
Subdivision 1 — Duties of designers  
Subdivision 6 — Duties of employers

**AS 1755 Conveyors -  
Safety requirements**

**AS 1418.1 Cranes,  
hoists and winches -  
General requirements**

**AS 4024 Safety of Machinery**  
Part 1604 Design of controls,  
interlocks and guarding –  
Emergency Stop  
Part 1202, Clause 5.11.8 Safety functions  
implemented by programmable electronic  
control systems

**AS 60204.1 Safety of  
Machinery –  
Electrical equipment  
of machines**

**AS IEC 61508 Functional safety of  
electrical/electronic/programmable  
electronic safety-related systems**

**AS 62061:2006 – Safety of  
Machinery – Functional safety of  
safety-related electrical, electronic  
and programmable electronic  
control systems**

**AS IEC 61511 Functional safety –  
Safety instrumented systems for  
the process industry sector**

**SA Gas Act 1997**  
Part 5 — Safety and technical issues

**SA Gas Regulations 1997**  
14—Installing or commissioning Type B appliances

**AS 3814-2005 Industrial and commercial gas-fired  
appliances**  
Formerly AG 501-2002  
Clause 2.26.2 Requirements for a  
programmable electronic system (PES)  
Clause 2.1.1 Appliance  
design

**AS 1375 – SAA  
Industrial fuel-fired  
appliances code**

